E-MAIL PHISHING SCAMS

1. Never share anything online you would not tell directly to the enemy.

2. Never post private or personal information.

3. Assume any information you share electronically will be made public.

4. Phishing scams tend to have common characteristics that make them easy to identify:

* Spelling and punctuation errors.
* Scare tactics to entice a target to provide personal information or follow links.
* Sensational subject lines to entice targets to click on attached links or provide personal information.
* Include a redirect to malicious URL's which require you to input usernames and passwords to access.
* Try to appear genuine by using legitimate operational terms, key words and accurate personal information.
* Fake or unknown sender.

5. When in doubt about a suspicious email from a supposed bank, call your financial institutions or check with your command Information Assurance (IA) lead. Your command IA can also assist with other types of suspicious email.

5 THINGS YOU NEED TO KNOW